THE STATE OF GLOBAL INTERNET FREEDOM

HEARING

BEFORE THE

TOM LANTOS HUMAN RIGHTS COMMISSION

HOUSE OF REPRESENTATIVES

ONE HUNDRED AND ELEVENTH CONGRESS

FIRST SESSION

JUNE 18, 2009

Available via the World Wide Web: http://www.tlhrc.house.gov

TOM LANTOS HUMAN RIGHTS COMMISSION

JAMES P. McGOVERN, Massachusetts, *Cochairman*

JAN SCHAKOWSKY, Illinois
DONNA EDWARDS, Maryland
KEITH ELLISON, Minnesota
TAMMY BALDWIN, Wisconsin

FRANK R. WOLF, Virginia, *Cochairman*

CHRIS SMITH, New Jersey
JOSEPH R. PITTS, Pennsylvania
TRENT FRANKS, Arizona

HANS J. HOGREFE, *Democratic Staff Director*
ELIZABETH HOFFMAN, *Republican Staff Director*

C O N T E N T S

WITNESSES

THE STATE OF GLOBAL INTERNET FREEDOM

THURSDAY, JUNE 18, 2009

HOUSE OF REPRESENTATIVES,
TOM LANTOS HUMAN RIGHTS COMMISSION,
Washington, D.C.

The commission met, pursuant to call, at 10:49 a.m. in Room 2226, Rayburn House Office Building, Democratic Staff Director Hans Hogrefe, presiding.

Mr. HOGREFE. I would like to welcome you on behalf of the Tom Lantos Human Rights Commission. I told you already about the voting situation, so, you know, I will take the testimony and share with the members, and we also will have questions and answers for you if you agree that we can go into afterwards. I still would like for you to go through your opening statements as you had planned, and then, you know, we go through questions and answers.

The hearing today comes at a very crucial time for two reasons I think. One, obviously, because it just behooves the Tom Lantos Human Rights Commission to continue its work on the internet freedom issue in China because it was the Conventional Human Rights Caucus in February of 2006 that was the first congressional entity to have a hearing on the whole issue of internet freedom in China and featured and brought congressional attention to the case of Shi Tao, who most of you are obviously familiar with, the Chinese journalist who was detained, arrested and convicted based on information made available by Yahoo identifying him as the holder of an e-mail account that had sent critical e-mail messages about an upcoming Tiananmen Square Anniversary to a pro-democracy website in the United States.

And our congressional hearing of the Congressional Human Rights Caucus then was followed very shortly after by the very first committee hearing. It was a joint committee hearing held by Congressman Chris Smith, who is the author of the Global Online Freedom Act, and this bill is pending currently still in this Congress before the House Committee on Foreign Affairs.

This was in 2006, and then there was another hearing before the House Committee on Foreign Affairs in 2007 that really followed up on the situation of Shi Tao and what Congress can do to protect internet freedom and also obviously in light of the legislation that was proposed by Congressman Chris Smith in the last Congress as well.

Today's hearing, obviously as with everything internet-related, internet freedom-related, has its starting point in China, but unfortunately we see that the Chinese technology, know-how and all this is exported. It is almost like a little cottage industry that the Chinese have developed to export their technologies, their internet strategies to other countries that have joined since then the club of what the Reporters Without Borders called the enemies of the internet, and I think that is a very appropriate name if you look at the consequences that their strategies, their government interference, their laws have on the lives of individual people because this is not just an academic discussion about proxy servers and encryption, email encryption, all that, although that is a very important part of it. But it actually impacts peoples' lives directly, and people are in prison because of that, and, of course, we know that there is not only the Shi Tao case in China, but there is also three other dissidents that are also internet writers or bloggers that pay the price for speaking out on the internet when they felt that they had a safe forum.

So having said all that, I will hand over the microphone or the floor to Elizabeth for any opening remarks that she may have, but I wanted to thank all of you for coming here, and I wanted to particularly mention Lucie Morillon, who is leaving tonight to return to Paris. Not only that she came and is pregnant and all that, what that implies, but

she also is going to be on a plane in a couple of hours to go back to France. I wanted to publicly acknowledge her role in the very first conventional event that ever happened on this entire issue, and that was Lucie's approach to Congressman Lantos, to Congressman Smith, her tremendous work that she has done on developing the Global Online Freedom Act as well as obviously with all her partners like Kumar and others, Harry and everybody else who is involved in this.

But Lucie was a steady and early voice when it came to internet freedom issues, and I am really grateful for all that you have done and I am really thankful for all your work, and I know that we will continue to work with Reporters Without Borders anyway even though you will depart and operate out of Paris, which is their gain and our loss. So thank you for everything, Lucie. Thank you.

[Applause.]

Ms. HOFFMAN. Thank everybody for coming and I apologize that it is us rather than the members. Unfortunately, 26 votes ensures that they are going to be out of pocket for quite some time, and I know particularly Mr. Smith wanted to be here, so we will be sure to pass the transcript onto him.

And in addition to China, I think it is particularly important to look at the global implications of online freedom, which is why we are pleased to have an expert with us today that studies Iran as the implications of online freedom have been particularly evident in the days following their elections.

So, without further ado, I am going to go ahead and introduce our first witness, Dr. Daniel Calingaert from Freedom House. He oversees Freedom House's wide range of civil society and media programs. He is also a professional lecturer at American University where he teaches courses on democracy. We are very pleased to have him with us today and look forward to his comments.

STATEMENT OF DR. DANIEL CALINGAERT, FREEDOM HOUSE

Mr. CALINGAERT. Well, thank you, Elizabeth. Thank you, Hans. I very much appreciate the opportunity to speak to you today about the growing threats to internet freedom around the world. The internet and other digital media have expanded space for citizens to express their views freely. In response, repressive regimes have employed increasingly diverse and sophisticated controls on the internet. These regimes have strengthened their ability to censor content online, to monitor internet users and to collect personal data, which they use to intimidate and prosecute their critics.

Over the past few days in Iran we were reminded of the threats to internet freedom but also of the internet's great potential. Following the June 12 presidential election, the Iranian government intensified its internet filtering. It also disrupted social networking sites like Facebook, and it jammed transmission of SMS text messages on mobile phones, and this was all an effort to prevent citizens from voicing their frustration and from organizing protests.

Nonetheless, Iranians were still able to use digital media to get news and photographs and videos out of the country. They were using Twitter but also other technologies that circumvent the censorship.

In April, Freedom House released a report entitled ""Freedom on the Net" and we have a few copies here and it is also posted on Freedom House website. This report develops a new methodology for analyzing and tracking internet freedom, and we applied this methodology to study 15 different countries in different regions. We looked at a very broad range of factors within three broad areas. We looked at obstacles to access to the internet, we looked at controls on content and we examined violations of user rights.

Each country is scored on a scale of zero to 100 and then is assigned into one of three categories: free, partly free, or not free, and it is similar to the ratings we use for freedom in the world and for freedom of the press.

The countries that are rated not free, such as China, Iran and Tunisia, use sophisticated systems with multiple layers to control the internet. They have systematic technical means of filtering. They also have human censors that monitor blogs and online forums and manually take down material that is on forbidden subjects like human rights abuses or corruption.

They block Web 2.0 applications like Facebook, YouTube, BlogSpot. They outsource censorship and surveillance to private companies. In other words, they turn to internet service providers, to blog hosting companies, to cyber cafes, to mobile phone operators to enforce some of the filtering and some of the surveillance. Cyber cafes, for example, in China and elsewhere have to check the identification of customers and they have to install software that monitors and filters the web browsing.

Non-free countries also manipulate online content. For instance, in China, you have the so-called ""50 Cent Party", who are paid commentators who are essentially there to disrupt or drown out online discussions that are critical of the government. They also have extensive surveillance of internet and mobile phone communications, and in addition to all the technical means, there is old-fashioned repression that bloggers and online activists are subject to harassment and intimidation and arbitrary arrest and worse.

So through all, we put all these different means together and you see multiple layers of restriction and control on the internet.

We were able to study only 15 countries in this initial study, but I think we would see similar patterns in other parts of the world and much more broadly. We know through the Open Net Initiatives research, for instance, that political content is filtered in a number of countries in the Middle East, in the former Soviet Union, in Southeast Asia, even in Africa, for instance, in Ethiopia.

In the partly free countries, such as Egypt, Malaysia and Russia, the internet provides much more space for free expression than traditional media. In fact, for freedom on the net, we use the same rating scale as we do for freedom of the press, which

focuses more on traditional broadcast and print media, and you see quite a big gap in scores for countries like Egypt and Russia, to show that there is much more space on the internet.

The censorship tends to be limited and targeted in these countries, but you shouldn't be at all complacent. We think that the space for free expression in these countries is closing, and there is extensive monitoring of internet use. In countries like Russia, you do have what they call the Red Brigades, which is their equivalent of the paid commentators there that promote the Kremlin's line, and there is much more reliance on penalties for individual bloggers or activists.

Egypt is a great example. There really is very little technical interference with the internet, but there have been a few prominent bloggers and online activists who were arrested and treated very badly, and that sent the message to other online users.

It is important to note that European and U.S. technology continues to contribute to internet censorship and surveillance. In April, there were news reports that Nokia Siemens Networks delivered an electronic surveillance system to Iran Telecom, Iran's state-owned telephone company. This system allows authorities to tap mobile phones and to monitor electronic data transmissions, and it is believed that this system can target dissidents.

In a separate case, which was reported last month, a city library in Mississauga, Canada, was found to use web filtering software similar to that in China. So basically a user going to this library in Canada was browsing sites dealing with the controversy surrounding the 2008 Olympics, repression of Christians in China, other topics that are banned inside China, and they were blocked on the library computer in Canada.

This was software that was sold by the company, U.S. company Websense, formerly SurfControl, and what it seems to indicate is that the company is using default settings or using basically a standard filtering made for the Chinese market, but that just becomes the default that gets sold elsewhere.

What should the U.S. do about this? For starters, I think at a minimum U.S. policy should ensure that companies will no longer be complicit in violating the rights of internet users, and that is why the Global Online Freedom Act is an important component of protecting internet freedom globally.

But GOFA is not enough. I think because the internet is so diverse and the censorship and controls in repressive countries are multilayered the response has to deal at many different levels. We think the State Department should intervene on behalf of U.S. companies that come under pressure from China or other countries to help with censorship or surveillance. We think the State Department should be more rigorous in challenging violations of internet freedom but also in building coalitions with other democratic governments to advance online freedom.

The U.S. Trade Representative should explore possibilities to challenge internet censorship as a trade barrier, either in bilateral negotiations or multilateral negotiations or perhaps as challenges before the World Trade Organization.

Congress should expand its efforts to press for greater internet freedom, for instance, to draw attention to human rights abuses against internet users, for instance, as Congressmen Barney Frank, Trent Franks and Mark Kirk have done in the case of the Egyptian blogger, Kareem Amer.

And the U.S. Government should provide support for activists and bloggers in countries where the internet is restricted, and perhaps it could challenge other democratic governments to set up a multidonor fund so that there is a shared commitment and greater resources in this effort, and this fund could support a number of things: education exchanges, advocacy by activists within repressive environments, also support and create networks between activists so that say the activists in China and Iran and others can learn from each others' creativity.

It is important to support more research on internet governance issues and also the development of innovative technologies to circumvent censorship and to protect personal data.

We think the combination of these can really put the U.S. in a leadership position in dealing with internet freedom, and this is critical at a time when the risks to internet use are growing. Thank you.

Ms. HOFFMAN. Thank you very much for your testimony. I am going to go ahead and introduce Lucie Morillon from Reporters Without Borders. She is the Washington, D.C. Director. This is her final act as Washington, D.C. Director of Reporters Without Borders, and, unfortunately, as Hans mentioned, she will be leaving us for Paris, but we certainly hope to continue to work with her from afar, and we will continue to work with the D.C. office of Reporters Without Borders, and we look forward to your testimony.

STATEMENT OF LUCIE MORILLON, REPORTERS WITHOUT BORDERS

Ms. MORILLON. Thank you. Thanks for your nice words, Elizabeth and Hans. It really means a lot to me. I also want to recognize the leadership of this Commission of the U.S. Congress on the issue of internet censorship and corporate responsibility. I would like to thank this Commission for giving me today the opportunity to present this testimony on the global trends in internet censorship.

These past days the events in Iran have been a reminder of the importance of alternative sources of media in closed societies. Some say Twitter has been to the Iranian events what CNN was for the Tiananmen massacre in 1989, a platform to reach the rest of the world. It illustrates the growing influence of online social networking services as a communication media, a media that has been used by the opposition but also citizen journalists and human rights activists to unify their supporters and also get their messages through while foreign media have been faced with restrictions by the Iranian government.

The internet offers tremendous potential for openness and freedom. In heavily censored countries, it has provided the space for discussion and debate that has been nonexistent or limited in mainstream media or society. It challenges authoritarianism, empowers individuals as never before and bolsters the exchange of information that makes an important difference in peoples' lives.

Traditional media organizations have not always been able to expose human rights abuses in specific countries. In 1988, the world received little notice of the riots occurring in Burma and the military regime's subsequent violent crackdown on demonstrators. News of these events only reached most Western countries days, weeks, even months after they occurred. With the help of the internet and nontraditional media, the blatant human rights abuses that occurred during Burma's 2007 Saffron Revolution were widely covered. Compelling YouTube footage often filmed by citizen journalists on cell phones or inexpensive low resolution cameras was conveyed around the world, sparking international outrage while the Burmese authorities ultimately shut down the internet in order to continue the crackdown unabated as the news was already out.

In China, activists and regular citizens have been using the internet to discuss issues such as consumer rights, social rights and environmental concerns. The blogger, Zilla, for instance, has become a spokesperson for the conditions of Chinese workers and has compelled the traditional media to follow his lead and stop ignoring this topic. As a result, the internet has been responsible for improving the quality of traditional news media coverage.

Internet users in China also criticize distribution of aid after the Sichuan earthquake, and the cause of mass organization ultimately forced the Chinese authorities to address the issue at hand.

In Saudi Arabia, women enthusiastically took to the internet and were able to express themselves freely and discuss health issues until the authorities claiming to be fighting the promotion of pornography blocked them. Breast cancer, for instance, is

blocked in Saudi Arabia. In Egypt, policemen were also prosecuted after a video circulated on the internet showing them torturing a suspect.

But not only a space for expression, the web has also become a means for action, particularly through social networking sites. In Egypt, these websites have taken on the role of trade unions which have been bound under the state of emergency in place since 1981. Active internet users create virtual rallies that give rise to genuine political demands. One group created on Facebook boasts more than 65,000 members and was used to channel protests in April 2008, calling on Egyptians to stay home. It contributed to a general strike and one of the largest expressions of civil unrest in several years.

In Iran, the fight for women's rights insufficiently covered by the traditional media was also taken to the internet with an accompanying one million signatures for the abolition of discriminatory laws against women, and this has ensured this campaign high visibility on the international scene.

The demonstrations that followed the Iranian presidential elections have also been widely covered on social networks. Anyone wanting to follow the situation closely had better read blogs, watch YouTube and keep an eye open for many filing Twitter updates from a country with a young and internet-savvy population.

The media involvement grew in response to the lack of coverage from the foreign media, especially at the very beginning of the crisis, and it eventually helped coordinate the opposition's demonstrations.

While the government tried to limit communications, new kinds of social media and technical innovations are allowing Iranians to find new ways around the restrictions. Iran's election was the top Twitter trend of the day last Monday, June 15.

Representative governments have fought back against local governments using different tools to silent dissidents. At least three dozen countries are currently involved in some sort of internet filtering and censorship these days. I am not going to get too much in detail because Daniel has addressed most of them, but some countries have set

up a very sophisticated system of internet censorship and filtering, China being the world champion of such tactics.

Today, 68 cyber dissidents and bloggers are currently in jail for expressing themselves freely on the web, some of them sentenced to more than 20 years in prison. Legal proceedings have been used against bloggers, sued for endangering national security, libel or insulting a head of state. Governments have also used the internet to spread misinformation and propaganda. The example of the ""50 Cent Party" is one of the best of the best ones.

Reporters Without Borders issued a list of internet enemies last March that include Burma, China, Cuba, Egypt, Iran, North Korea, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan and Vietnam, plus a list of countries under watch, and these countries have been able to transform the internet into a new trend, preventing users from posting views seen as undesirable.

However, bloggers and internet users have proven to be resourceful. For instance, they will often misspell a key word they know is censored in order to avoid having their post deleted. This is one of the reasons why the Chinese authorities today end up blocking about 500 words that are related to Tiananmen Square.

Internet users also use metaphors and humor to get their message through. The term ""River Crab" was created by netizens in China in reference to internet censorship. In Mandarin, it sounds very similar to the word harmonious, and the Chinese Communist Party announced the goal of constructing a harmonious society, which has been actually an excuse to delete negative news. So when Chinese netizens use the name ""River Crab", what they want to say is that they are describing the actions of blockading and concealing negative news.

Internet users employ proxies of software and technologies such as Freegate, VMP, Tora or Siphon to pass by censorship. According to *The New York Times*, the Global Internet Freedom Consortium, an internet proxy service disguised as a banned

Chinese spiritual movement, Falun Gong, offers also download-labeled software to help evade censorship that is being used in Iran right now.

And in countries where existing use is present, it is not unusual to find software to defeat online censorship already installed on computers in cyber cafes and also cyber cafes' managers helpful to show you how to use it. Once censors have identified proxies, new ones have become available in most instantly transforming internet users to a constant game of cat and mouse between government and citizens.

Human rights defenders should remain very vigilant about visitor blockings and not take internet freedom for granted. Some governments invest a lot of resources in internet censorship and not everyone is text-savvy or curious or able to go around internet censorship and make the effort to find the relevant information.

Repressive governments such as China have made their jobs easier by enlisting the help of Western companies to control the internet. Yahoo and Google have since sought the reserves of the Chinese version of their search engines to remove containments sensitive by the government, and Microsoft has installed a Chinese version of its block platform.

Yahoo has gone further than other companies and given some personal identifying information on users to the Chinese authorities that has allowed them to identify and convict at least four dissidents who expressed themselves freely on the internet. One of them is Shi Tao, you mentioned it earlier. You know, when dissidents initially choose a web mail-based email account, they should be entitled to better privacy protection from a multinational company than the local ISPs directly controlled by the government.

One of the demands of Reporters Without Borders is we have been asking IT companies not to have their e-mail servers within internet-restricting countries to avoid being forced to reveal the identity of their users.

The next challenge for the companies are going to be Vietnam, more countries like Vietnam. More than 80 percent of Vietnam users are hooked up to Google and Yahoo rather than to domestic platforms, and the Ministry of Information and Telecommunications is planning to put forward corporation proposals to regulate the content of blogs using foreign companies' platforms, and under this provision they would have to accept to provide information from their customers. So the next Shi Tao may very well be Vietnamese.

China has gone one step further recently in announcing its internet censorship system. It announced earlier this month that personal computers sold from July 1 must carry internet filtering software preinstalled by the manufacturer, actually allowing the government to spy on individual users and preventing them from accessing an ever-changing list of banned websites. Concerns have been expressed that the software is full of flaws that could expose users to hackers able to steal personal information.

Western PC manufacturers have since asked the Chinese government to reconsider its decision and the Chinese blogosphere has been adamantly commenting on how to deactivate the software. It would be great to see U.S. computer makers lending them a hand.

Despite resourceful netizens, the fight for a free internet is far from being won in front of powerful governments ready to implement Big Brother-like policy. Concrete measures should help sustain the effort of cyber dissidents in closed societies so that the internet can remain an open window to the world when all the other windows have been shut.

Here are our recommendations: The U.S. authorities should allocate more resources to groups who are drafting secure technologies to bypass internet censorship, and the U.S. Trade Representative should also work on building an alliance of countries that would raise the issue of internet censorship before the WTO, considering that the lack of information to censorship is a barrier to free trade. Congressional hearings should

also be held as soon as possible with American PC makers to discuss new regulations, especially how to avoid implementing these repressive measures, and take a look at the claims that Green Dam software contains pirated code from a California company, and Congress should also continue holding hearings about Western companies collaborating with internet-restricting countries, especially since representatives of companies such as Cisco System have not joined in the industry discussion that led to the creation of the Global Network Initiative, and last but not least Congress should pass the Global Online Freedom Act introduced by Representative Chris Smith as soon as possible. This bill aims to prevent American companies from cooperating with repressive governments in transforming the internet into a tool of censorship and surveillance. Reporters Without Borders is also working with the European Union on a similar initiative, and we consider that today it is actually a significant advent for online free expression and would be the best way to avoid another Shi Tao case.

Thank you for your time.

Ms. HOFFMAN. Thank you very much for your testimony.

I would now like to introduce Mr. Harry Wu, who is the founder and executive director of the Laogai Research Foundation and played a critical role in bringing to the attention of the U.S. Congress the Shi Tao case in 2006. Thank you very much for joining us and we look forward to hearing from you.

STATEMENT OF HARRY WU, LAOGAI RESEARCH FOUNDATION

Mr. WU. Thank you. Ladies and gentlemen, I come to this Commission talking about the China issue. Just as you know, China is the most important country in the world today. They have 22 percent of the population of the world, and as economy is growing and particularly this country, the government actually, is owed many billions money of American bound. Anyway, this is a Communist Regime and to this moment in

this country there is no religious freedom, and all the women today, they are not free to give birth.

When American talking about abortion, a forced abortion, in China it is very common. Every woman is subject to the abortion because whether you are married or unmarried you cannot pregnancy if you don't have a permit from the government. If you have a permit, then you can make love freely and then make a child first, but that is it, one child per one family. The woman is not free to operate their rights.

Anyway, let us focus on the internet. Over the past several weeks the Chinese government has caused quite an uproar among its 300 millions also internet users. The most of the country in the world after the Chinese Ministry of Industry and Information Technology announced a decision to require that all computers sold within the country from

July 1 onward be preinstalled with so-called Green Dam Youth Escort.

But I am not going to be talking about the detail about the software, the situation. The Chinese government just yesterday make a new announcement that she said the installation of the software is optional. So Chinese back up.

While the outcries from the user and the computer manufacturer may bring such an issue to light, the real reason for the Chinese government change is because there are many flaws issues to light, the real reason and within the software, and that allows the hackers to take over the computers. But I don't think the Chinese government will give up its intention to control the internet speech. There is many other ways. Today China have probably 200,000 policemen, just internet police control the internet, and unfortunately many company, include the Google, Yahoo, and Microsoft, while just as they said we have the business inside China, so we have to follow Chinese law.

Well, I just want to say if the business in Soviet Union, if you are going to follow Soviet Union law, you would not, right? So it is only the model issue, but it is a big

problem in the near future, you can see that because Chinese is using the internet not only for international but also for domestic politics.

China has already developed the most advanced police state in the world, and if implement plan Green Dam would significantly supplement its capabilities in the software world and add a new layer of censorship, operating at a level of individual computers on top of the network level censorship that already exists, which is commonly referred to as the ""Great Firewall of China".

The Great Firewall was developed in the late 1990s to control the censorship of Chinese computer shortly after internet came into China and was built to a large degree with technology supplied by Western company such as Cisco Systems, which sold the Chinese security the realty switches necessary to build a highly sophisticated system and also include Chinese program. They are training Chinese police to using the systems.

Cisco were later involved itself in the Chinese ""Operation Golden Shield" project, which aimed to develop a national civilian systems and database of citizen records that will be regionally accessible by the state and public security organs at a national, provincial, even the municipal levels. Cisco actively courted and signed contracts with different level of Chinese public security agency to develop some of these technologies. We have the press conference in the House, but until today, well, almost four years that really some people care about it.

A number of other U.S. technology company have also market high-tech civilian products to the security organs in China, including factual and voice recognition software and it could be very useful for the identifying of dissidents. Such sales certainly seem to violate this right if not the letter of the Tiananmen sanctions prohibiting the exporter crime control or detention instruction or equipment to China, which will enact through the Foreign Relation Authorization Act from the 1990-1991 fiscal year.

Last year I called upon the Department of Commercial, Bureau of Industry and Security, to update Commerce control list to include these kinds of high-tech civilian

products as to use technology and to take into consideration their end user. That means stop the repressive Communist Regime. But today I am unaware of my change have been made.

The Chinese government have produce assistance of U.S. company in restricting online freedom in other ways as well. Companies such as Yahoo, Google, Microsoft that have operate search engines inside of China have been complicated in featuring several results for insensitive content of the direction of Chinese government.

Notably, several years ago Yahoo even went so far as to turn over user information for several individuals inside China who used its service to publicize or transmit information critical of the government, and the most one of which is that you list Shi Tao. Until today Shi Tao was still in the jail, and she was sentenced to 10 years, that contribute to their being arrested and sentenced to long terms in prison even today.

Yahoo, which no longer operates inside China, but Yahoo own a large of the Chinese search engine alibaba.com, so far as I know more than 40 percent, has since apologized to the families of those individuals and offered them financial compensations. It also partnered with Google, Microsoft and others to create the Global Network Initiative, which aims to develop a shared approach for the companies or other stockholders to advance the freedom of expression and privacy in markets such as China.

Well, it is still unclear how other internet companies operating in China, including those have sign onto the GNI, will respond to the future request for using information made by Chinese authorities. That is why I have consistently advocate for the U.S. Congress to pass the Global Online Freedom Act sponsored by Representative Chris Smith, which will prohibit by U.S. company from complying with such requests except under limited circumstance.

Fortunately, the rollout of the Green Dam software has not proceeded as mostly as the Chinese community have probably hoped it would. In addition to the backlash for its own citizens, including many who plan to mount a legal challenge against the policy,

researchers at the University of Michigan and elsewhere have identified major security flaws in the software, and the government has order the Chinese company fix these errors now in what appears to be a major turnaround. We have learned that the government is now backtracking and making installation of the Green Dam software operation rather than voluntary.

But I want to say that in many years the internet has become the new battlefront for freedom and democracy in China, and sadly I feel it is war that the Chinese government is slowly winning. It has invested in massive resources into clean up the internet and acquiring and installing the most advanced firewall technology and also employing an estimated 30,000, 50,000 internet police to monitor the web, shutting down domestic blocks and websites and starting to take away business license from the serve providers that didn't censor content on their own.

Moreover, the more the Chinese public becomes aware that the government is monitoring them, the greater is their tendency towards self-censorship. As the Green Dam handover, even though it was not complete successful, I believe the Chinese government has already laid much of the underwire to replace it with a super system at some point in the future. Thank you.

[The statement of Mr. Wu is unavailable]

Ms. HOFFMAN. Thank you very much for your testimony, Harry.

We would now like to welcome Mahadi Khalaji, who we are very pleased to have from the Washington Institute for Near East Policy where he is a senior fellow focusing on domestic policy of Iran as well as the politics of Shia groups in the Middle East. We are very glad to have you as this is very timely as it concerns Iran and look forward to hearing your testimony.

STATEMENT OF MEHDI KHALAJI, WASHINTON INSTITUTE FOR NEAR EAST POLICY

Mr. KHALAJI. Thank you. As you said, the reason I am here is not that I am an expert on internet. It is because the ongoing crisis in Iran regarding the postelection demonstrations of people which started on Friday night and continues and now as we are sitting here, in Iran, in Tehran streets, a large demonstration is happening in favor of the reformist candidate, and tomorrow also people are expected to gather in the Friday prayer event, which is going to be performed by Ayatollah Ali Khamenei, the Iranian supreme leader.

All these events since last Friday was reported mainly through internet. Right after they closed the polling stations the government asked the majority of the foreign journalists to leave the country, and now in Iran we have few foreign journalists like Christiane Amanpour from CNN, and even people like Amanpour are not allowed to go to the street and they say to them if you want to report the events, you will have to report from your room in the hotel.

So there is lots of pressure on the journalists and even AP. You know that most of media, foreign media do not have any office in Tehran, but AP and Reuters, they have two large offices in Tehran, and there was a contract between AP and Iranian Government that if they got any photo or any film they are free to pass it to other media in the world. And BBC Persian TV, which was launched on January 14, was allowed to get film and pictures from AP and Reuters office from Tehran because they don't have their own office in Tehran.

But since Friday, government told AP and Reuters that they are not allowed to pass their photos and films to BBC Persian TV and Voice of America Persian TV. So the only way to report this event was to go through internet, and especially Facebook and Twitter were two main website, and YouTube of course, were three main website through which Iranian people could send pictures, news, video clips and so on.

Unfortunately, since Friday morning the government blocked Facebook and Twitter and YouTube and some other websites, but as people know how to deal with filtering in Iran, Iranians in general are creating always or designing the new software for breaking their filtering.

The State Department's request from Twitter to delay and postpone the maintenance in order to let Iranians to send their messages through Twitter was very significant and Iranians were very happy about it, and actually it helped a lot to send the message or the reports from Iran to the world outside.

Iran, as we assume here, many of us in the West assume here that is a government of clerics or a clerical government, actually is a government of juniors. It is a very digital government and even clericals or clerical establishment, which is separated from the government is very digital. One of the biggest digital center in Iran is not in Tehran, it is in Khonj and inside the seminary, and they have a center for information and computer studies, which is a source of creating lots of software in Iran, and actually what people say is that the capital of computer in Iran is Khonj, so they have held many exhibitions which shows that to what extent they are advanced.

In Iran, the Iranian population is 17 million, but 23 have 70 percent of population are under 30 years old, and we have in Iran 25 internet users and these 25 internet users are mostly young and under 30 years old.

The government who could not prevent internet to be popular in Iran started to block the websites and not only the website which are against the Iranian moral codes but also any kind of website inside and outside which criticized the government. They created even different center in the RRGC, Revolutionary Guard and Basij Militia as well as in the clerical establishment to pay some people to blog and post the comments on other peoples' blog, and as you know, the bloggers and the writers and journalists were under heavy pressure since 12 years ago, since the reform movement started in Iran.

Ironically, in Iran, what the government has done is that, for example, regarding a website like Facebook, the first reaction of the government was that they blocked it, they blocked Facebook and say this is against Allah because Facebook is a network that allows boys and girls to mingle, and this is against the Shia. For the same reason there is no Yahoo Messenger in Iran because people chat, and through chat they commit sins.

But after awhile the government suddenly decided to unblock Facebook, and the main reason was that they realized that through Facebook they can have better control of peoples' activities and know how people inside Iran are connected to the Iranians outside Iran and who goes where and does what and actually open Facebook in Iran was unblocked until Friday election, and I think that this is the ironic aspect of internet in Iran that made it easier for an autocratic totalitarian regime to have control over peoples' activities.

So I have got this report from different engineers in Iran who are working in the communication ministry that Iran is buying different technology for future from different countries, but one of the technology that they got from loan two years ago was a technology that allowed them to monitor all the e-mails and even the attached files, whether audio or text or anything.

So that is why people in Iran they do not even feel secure to communicate through e-mail or even attach files to the e-mails under surveillance of the government, and that is one of the things that shows that many companies in the West, they don't feel the responsibility or they don't feel enough the responsibility of what do I do in terms of trade and selling those sort of technology to a country like Iran which can be dangerous for the life of many people.

One of the measures that government is taking against the internet in Iran is that they limit the speed of internet significantly, so, for example, people in Iran, if you want to check your e-mail, for example, you spend three minutes here to check all e-mails, but they spend an hour to open three or four e-mails, or they are unable to download any

audio visual files, and it will be very difficult for them to work with computer and it will be very boring and actually one of the reasons that since four years ago SMS or the text message system became more popular than internet was the speed of internet in Iran.

You know, you could not spend lots of time with low efficiency on the internet, and too, for example, you cannot chat with it, you cannot open your e-mail. It was very difficult because the government made it difficult working with internet. The SMS became popular in Iran and actually became the main tool of the communication with the youth. And unfortunately since Friday the text message system is cut off too and people are not able to send message to each other.

The main concern now is that since more violence is expected in Iran in coming day and since two parties are not willing to give up and the government feels self-confident enough to crack down on people and demonstrators, they are planning to disconnect the internet in all the country, and now half of cell phones are disconnected, but if they want to have bigger bloodshed on the streets, they would cut off internet, cell phone and even possibly many of fixed phones and land phones.

So if we see today that BBC Persian TV or Voice of America TV, they are able to enhance the voice of demonstrations in Iran and put pressure on the government which wants to suppress the demonstrators, it is because of this internet. We are not free to use internet in Iran, but even the same low level of our ability in Iran to use internet allows us to enhance our voice to the world outside.

I think that the U.S. Government not only has to take some measure as my colleague here said, but they have to collaborate with European countries too and ask them to consider a technology trade with Iran to not sell them anything that would help them to suppress people, to reduce censorship on internet, to do surveillance of the people, even invade their privacy, privacy of people and be more responsible toward human rights and the moral values.

Thank you.

Ms. HOFFMAN. Thank you very much for your testimony. We now turn to Amnesty International's East Asia and Pacific Director, T Kumar, to speak a little bit about some other different initiatives that have been undertaken to combat censorship. Mr. Kumar, thanks for being here.

STATEMENT OF T. KUMAR, ADVOCACY DIRECTOR FOR ASIA & PACIFIC, AMNESTY INTERNATIONAL USA

Mr. KUMAR. Thank you very much. Amnesty International is extremely pleased to be here and we would like to thank the Tom Lantos Human Rights Commission for taking the lead, and as Hans mentioned earlier, you were the first ones as caucus to take the lead, so thank you very much and we are in a critical stage today because of what is happening in Iran, and before I start my presentation, I also want to join both of you to thank Lucie for the excellent work and her leadership.

When you come to internet censorship, it is the government that uses the new technologies to suppress freedom of expression by its own citizens, but there is a limit to it. How do they do it? They have the laws, they have the police, so with them, internet company sources join hands wherever they are allowed to operate. That is what has been so in China.

But in Iran, that is not the case because of the sanctions and other reasons internet companies are not there. If they were there, I bet they will join hands with them and join Iranian government to suppress the peaceful expression of what is happening out in that country. That is why the initiative on GOFA is important, the Global Online Freedom Act, so when abuses do exist the U.S. Government and U.S. Congress can react, but so far the reaction has been partition, not under Obama Administration, by the way, because it is too early to judge.

So I will go through quickly what has been done so far and what should be done. What initiatives have been done so far to counter what the governments are doing and to

counter what internet companies are doing, as Harry Wu mentioned, the main case that brought all of us to this table a couple of years ago was Shi Tao.

Shi Tao was a journalist. His I.D. was given by Yahoo, and to Amnesty International's record, he also recorded four other prisoners who were in prison because of Yahoo's involvement in identifying the user I.D. of journalists and political activists in China. But so far Yahoo did not take any actions to release them, and to our knowledge even Bush Administration did not take any first steps.

So the steps that have been taken can be divided into a couple of pools. First is the UN took a lead with what is called Global Compact, but again it is voluntary, so governments get off the hook. The internet companies get off the hook very easily. It is voluntary. Certainly some multistakeholder initiatives that again it has some value to it, but again internet companies as well as the governments can easily get over it because it is voluntary. That is why Amnesty International decided not to be part of it after two years working with internet companies and others to clear this voluntary initiative to see that it is going to work.

The third one is the U.S. Government initiatives. On Iran, they called the internet, how do you call it, Twister? How do you call it? Twitter, I mean by this to make sure it couldn't induce a further delay, Twitter to stop delay, whatever the delay they are servicing.

We hope to also take the same leadership in calling on Google, Yahoo and others to be more sensitive to human rights operations, so let us hope this is the first step that the State Department have taken, let us hope they will open it for other corporations and other companies to put principles in front above profits.

Then U.S. Government, first the Bush Administration, then we have the U.S. Congress, that is where Congressman Smith's initiative on Global Online Freedom Act comes into play. It is an excellent initiative. It was introduced to them in the last session of the Congress. Two groups of people worked intently to block it and defeated it.

The first group, Bush Administration, State Department, sorry, Justice Department and State Department both convicted to Congressional leadership that if you pass this initiative, this particular bill, it is somehow going to make it difficult to have diplomatic initiatives with other countries. It is such a shameful stand the Bush Administration took.

It was reintroduced this year, and now we hope President Obama's administration doesn't follow Bush Administration footstep in trying to block it behind the back. That is a challenge that we all want President Obama to take and take the leadership and support this initiative. If his administration fails, we will be sad to say that at least on internet freedom President Obama's administration will be no different than President Bush's administration in caving to big money and corporations.

The second thing that destroyed Global Online Freedom Act during the last session of the Congress was internet companies. They were all over the place. Their lobbyists were all over the place, to the extent of coming and pressuring us. Even NGOs they were pressuring. They succeeded. So we hope the U.S. Congress does not back off to the pressure of internet companies because this issue is more than internet companies or profits of U.S. corporations. This is about lives in other countries that is being played out at this moment in Iran.

So we are going to see many Irans' coming up if U.S. Congress doesn't act that will be supporting Global Online Freedom Act with 100 percent strength to make sure that U.S.-based internet companies have some restrictions in giving identities of those who use their accounts.

The second one, which is right now taking place in the U.S. Congress, is the foreign ops bill for the State & Foreign Affairs part of it. There is a section called Democracy Fund, which, of course, it was written before Iran blew up. There are $15 million that is being sought to help technologies so that it can use to all accounts the governments trying to block it. So we are urging the international authority and U.S.

Congress to make sure that particular initiative passes because that helps funds available to make sure that internet blockades around the world is taken care of.

The last initiative is a very interesting initiative. It is a group of individuals or NGOs who got together and started with Global Internet Freedom Consortium, in short, it is GIFC. What they do, they create counterissues to the government initiators to unblock it so they have it in their papers. I thought that even a lot of Iranians are using it now. It started because of Falun Gong issue in China, but that is the initiative by individuals and NGOs who started it. That is a saving grace now.

So the NGOs have taken the lead, but corporations are not helping it, and U.S. Congress so far, at least until last December, was not helping. So that is where we stand. That is where our challenges are enormous. As we are seeing in Iran, it is a second wake-up call to all of us. The first wake-up call was in China when Shi Tao and others were imprisoned and internet police was going around arresting people and imprisoning them. We should not wait for the third wake-up call. It can be done right in the Congress and right by the Obama Administration.

Before closing, I would like to touch on Iran -- because obviously that is in the news. Iran is not the only country that is blocking and abusing people who are using internet freedom. Egypt and Saudi Arabia have good company there with the Iranians. So U.S. Administration and Congress should be very careful not to take partisan view and attack Iran alone. They should realize that their own friends, Egypt and Saudi Arabia, are also champions in abusing internet freedom. If they take partisan view, it becomes political issue, not a human rights issue.

And on Iran, Amnesty International, we checked with our London office today. As of yesterday our website was not blocked. Amnesty International's website was not blocked. It is strange what is happening in Iran. Mr. -- would be able to shed some light because he is an expert, but we see blocking of internet access was kind of across the board although before this crackdown started, reporting to OpenNet Initiative, they

reported that across the board they basically blocked it. They blocked secular politics and reformist viewpoints. These are the majority of the blocks that were blocked, but however they also blocked, how do you call it, blocked several deemed to be too extreme. They also blocked some extremist Islam blocks.

So we don't know what is happening there, but at least from this OpenNet Initiative, the effort is even-handed in blocking both sides of the spectrum, but what we are seeing today is they are trying to block anyone who is trying to send information overseas.

So our challenge to the NGOs and the challenge to the Congress is to make sure that we pass this bill, Global Online Freedom Act, and to allow the $15 million that have been asked in the Foreign Ops Appropriations, and the biggest challenge is more than this. It is that internet companies themselves not become friends of the oppressive societies. Instead of becoming agents of change, they become agents of oppressive governments. The final challenge is for President Obama's administration to wake up and move fast to ensure that internet freedom is free everywhere. Thank you very much.

Mr. HOGREFE. Thank you very much, Kumar, and thanks to the entire panel for your outstanding testimony. With your permission, I would like to go to a couple of rounds of questions between Elizabeth and I if you would indulge us because I think we still have a little bit of time left.

Let me first of all start out with following a line of questioning that goes along the lines of some of the testimony that you have done before we go into specific aspects of questions that we may have.

As you know, I mentioned the history of the hearings and some of you mentioned this as well in Congress and congressional action. As one of the results of congressional interest, Secretary Rice had announced on February 14, 2006, the creation of a State Department task force which had the great acronym GIFT, and it was a lucky gift to us I guess, which was called the Global Internet Freedom Task Force.

It is unclear at this point what the exact status under this administration is of this task force, and we haven't been really able to verify this, but no matter what the status is, do you on the panel believe that that was a successful initiative? How would you evaluate this initiative?

And the second question goes to the other initiative, the other really main initiative that resulted out of the hearings, which was that of course the internet companies have tried to come together to develop a Code of Conduct, GNI, the Global Network Initiative, and which in 2008 I believe it was, in June 2008, after lengthy discussions that Kumar alluded to, agreed on three core documents on which the entire network is based basically, the network initiative. How do you evaluate that? I mean, what do you think about this particular initiative? And this is an open question to all of you to comment on both aspects.

Mr. CALINGAERT. If I may start, I think both initiatives are commendable but nowhere near sufficient. The Global Network Initiative, I would agree with the other panelists; because it is voluntary I don't think it will ultimately be successful when companies come under pressure from the government of China or others to turn over personal data, and that is why you do need legislation like the Global Online Freedom Act, so that the attorney general gets involved and can decide if a request for information is a legitimate part of a criminal investigation or is it an effort to get at dissidents.

The State Department's Global Internet Freedom Task Force I think is an important initiative and there were important resources behind it, there was support, among other things, for anticensorship technologies, but it doesn't get at really the scale of the problem and the diversity of the problem.

Going back to my testimony, supporting anticensorship is just one piece of the puzzle. I mean, I think you need to get at this problem many different ways. I should add one of the things that I think is very valuable in GOFA is this idea of exploring export controls, that the same way we look at curbing dual-use technologies that might be

used for military purposes, we should do the same for technologies that might be used for human rights abuses.

Even then that only deals with U.S. companies, and it doesn't help if we are enforcing good behavior by U.S. companies and then European companies turn around and sell those very technologies.

One important point about how to address this problem, the anticensorship technology gets a lot of attention, and I think it deserves that attention, but that is essentially helping communication from inside a country like Iran or China to the outside world. A lot of the important content is generated inside. It is Iranians putting up their own blogs and communicating with each other, and the anticensorship doesn't necessarily get at that problem, and so it is important to find ways to support activists and bloggers within these countries who, you know, they are quite creative and resourceful and they find ways to get around censorship, and so the more we can empower them and especially help them learn from each other, I think there will be a bigger impact.

Ms. MORILLON. Regarding the State Department Task Force, I mean, it was definitely an interesting initiative on paper. Now, as far as I remember, we had two meetings. There was a real problem of follow up, and nothing really concrete came out of it. I mean, we need to see a real political wheel behind this kind of initiative; otherwise, it is not going to be useful if it is just to say that we check the box, we sit down, we discuss the issues, and that is it. This is not what we expect from State Department.

And I think the fact that the State Department has now reached out to Twitter and so on can send a signal that the new administration is ready to go forward on this issue. So another State Department task force, yes, but with a real agenda and a real political role behind it.

Regarding the Global Network Initiative, Reporters Without Borders was involved in the negotiation with and probably participated for about two years, and eventually exactly like Amnesty International, we decided not to sign on the principle

that the GNI drafted, and one of the reason is, I mean, on one hand we recognize it is a positive initiative, it is the first time that the companies were actually recognizing the fact that there is a need to defend freedom of expression on internet, but on the other hand we just felt that it was not going far enough because it is a voluntary process and some of the language had been watered down. We would like to see stronger language in terms of resisting government requests, and also it was unclear how the process of monitoring the application of these principles would be in the coming years.

So again we do not want to be closing the door, it is an interesting initiative. We continue to follow it, but as the companies mentioned during the 2006 hearings, it is also a government-to-government issue, and the Global Online Freedom Act in placing the Justice Department as a sort of referee between the government requests and the companies' response is also helping to address the issue.

We can understand. We are not expecting the companies to resist individually, but if we have the U.S. government step in and saying no, under U.S. law you cannot give this information, then it would give the companies real tools that they can use to refuse to comply with some of the requests from governments looking for personal data.

Mr. KUMAR. Yes. First on the State Department initiative, GIFT, under Secretary Rice, let us be honest. Secretary Rice did not wake up overnight and say let us fight for internet freedom. The reason why it happened, because we were all involved in that, was Shi Tao was arrested, there was an uproar in the Congress. There was a hearing that involved Tom Lantos and a series of hearings. So much anger in the Congress and in the country, and they were at that time ready to move legislation, very strong legislation, so they stepped in to basically protect not freedom of expression, protect the internet companies. That is my read of it.

We attended meetings. Lucie was there a couple of meetings. We attended meetings. There were open discussions, but they also went behind our backs and came to the Congress and created another global bill. You know there were competing bills at

one point. We know that they played a destructive role rather than a constructive role in protecting internet freedom by the State Department.

That is why it is important that now Obama Administration should take a new initiative. They can have the same name, GIFT, but play a constructive role in supporting Global Online Freedom Act as well as being the real champions in fighting for the internet freedom around the world. Thank you.

Mr. HOGREFE. I know that some of our witnesses have to leave and you are excused if you have to leave at any point in time.

Do you have any particular question for them? Okay. Then you are excused to leave. Thank you very much for your excellent testimony, and we will share it with our members of course.

Let me ask you one of the things that I don't think has been really fully explored is -- well, okay. Overall an internet censorship, as I understand it from a technical point of view, and please believe me I am not a computer expert, and that will become apparent in the next sentence I am going to tell you, but apparently there seems to be different approaches. The most I guess brutal approach is that you control that access point to the internet that a company can provide, the ISP provider, right, the internet service provider, where you log in and you can have a government-controlled entity provide the internet and that is the only legal access to the internet that you can get where you physically make the physical connection, where you get the service.

That according to some expert reports I read seems to be the easiest but also very effective way of controlling it. But on the other hand, to me, it also seems to also be clearly a trade issue.

Why is so little of the discussion focused on that this should actually be a WTO aspect that we bring up, that our internet companies are here doing business from providing that, and if we join forces and if that aspect were maybe clearer to internet companies, they can throw their significant weight behind this I would suppose, because

believe me members of Congress hear every day from companies when they think that they don't have equal ground for competition in another country.

Why has that not happened here? Why do we simply say, oh, well, you know, they only allow one company in the entire country to provide internet. Why is that possible, and why do we not say one thing about that, or have we said one thing about it and I have just lived under a rock and have not heard about it? I would be interested in hearing what you have to say about that.

Ms. MORILLON. Well, I guess that is one recommendation, and I think it is yours as well, that this issue should be raised with the WTO. It is probably better if it is not raised only by the U.S. but also by a group of countries that do share these concerns. We kept saying that internet censorship is a barrier to free trade whether it is because you need free information to be able to assess your investments, because it is important also for businesses to be able to have access to report on corruptions and so on that sometimes are exports on the internet but nowhere else.

So, yes, that is something that should be explored more by this administration, and we will definitely support such an initiative provided that it is a multinational initiative.

Mr. HOGREFE. Any other comments? Have any of the NGOs had any conversation with the USTR, for example, the U.S. Trade Representative about that?

Ms. MORILLON. I think some of our people in our headquarters have been working on this, but I don't have the specifics, and I am happy to get back to you on this later.

Mr. HOGREFE. Okay. That would be wonderful.

The other thing that has come up in this context is of course our support, and you mentioned this also with regards to the GIFT initiative, that we make monies available or resources available for counter surveillance purposes on the internet, basically technologies, and these are government-funded initiatives I presume, and we obviously

are -- the most famous example that is always cited is the Falun Gong technology that they developed and all that, which I think is great, but that can hardly be the responsibility of a spiritual group to help solve the internet problem.

Why aren't our big companies not doing more in terms of developing these similar technologies? Of course I understand that they have to be easy to use, and it is clear that people have to also have a certain amount of trust in the software that they have been sent because they put their faith ultimately on that software, and, you know, if it is from another Falun Gong member, presumably there is a little bit higher trust level than if it comes from Microsoft or something, not to single out Microsoft, but they have more of a connection, more of a trust.

But still that doesn't mean that the companies should just stay out of it. What are their efforts in helping to develop this? Anyone please?

Mr. CALINGAERT. There are two parts to the answer. One is, for the anticensorship technology, it really is a nonprofit enterprise. I mean, the people who want to use it are users in China or Iran who don't have a lot of money to spend on this, and I don't know, under sanctions, they probably couldn't pay the U.S. company to buy this technology. So it really has to be publicly funded or through private foundations, and given the cost and the scale that we are trying to develop this, I think it needs public funding.

For the companies, there are better practices by some companies than others. For instance, Google has a secure log-in for its e-mail and for its other services. So there is a certain amount of security and protection for users anywhere in the world. Others, my understanding Yahoo does not have that, and Facebook does not have that, and in the case of Facebook, it is a real issue because the cases we were talking about from Yahoo got personal information on individuals. With Facebook, you have networks, and networks are great for mobilizing, for spreading the word among democracy activists, but if an oppressive regime gets its hand on that, they are not just going to get the individual

activist, they are going to get the whole network, and Facebook doesn't have that protection.

So I think part of the response should be encouraging companies to promote best practices, and there are things that they can do to at least improve the security and the privacy of their users.

Ms. MORILLON. I agree, and I think it would be an amazing question to ask a representative of a company in a follow-on hearing.

Mr. HOGREFE. Are there any other responses?

Let me just clarify, I did not mean to suggest by my question that there shouldn't be public funding or that the internet companies should pay for it. What my point of view is is that given that they are the service providers and let us face it, there is significantly more computer expertise with Microsoft and Google and Yahoo and Facebook and Twitter and all that than in the U.S. Government because that is an all job, that the ideas and technology should be developed there and that of course the government should help to pay to develop these technologies because they are obviously not going to be particularly commercially viable products because, as you say, it is for a certain group of people that would use it.

But I think that they almost must be in a perfect position to figure out what could be done to counteract the efforts because they also know what their weaknesses are and having their products controlled. I mean, you know, it doesn't get any better than that than the resources in Redmond and all that where all the research development people sit, you now, they know what is going on and how the Chinese do it or the Vietnamese do it or the Iranians do it, and they can figure out, okay, but there is a back door to countering that. That is just a thought.

Do you have any questions?

Ms. HOFFMAN. Just one really and then we are out of time. I was wondering if you could elaborate a little more on companies that do have best practices and which

companies we should really target in improving security of personal information and could be encouraged to join GNI and groups like that. I know Twitter is a relatively new phenomenon from what little I do know about it. They seem to be pretty good in protecting personal information and free flow of information. I was wondering if that is true or false.

Ms. MORILLON. I won't be able to answer in detail for Twitter because we are actually looking at the issue, but, I mean, there are definitely two different issues here at stake, which is the protection of personal data and the issue of censorship, filtering and so on.

Regarding the personal data, we obviously want to keep a very close eye on what Yahoo has been doing because even if they have joined GNI, even if they have created this film to help support some cyber dissidents and so on, they still don't have operating power in China, and they work with Alibaba, who they keep telling us we are not responsible for what Alibaba is doing and so on. Still they are using their brand name in China, so there should be some sort of responsibility here. So Yahoo is definitely a company you want to keep a very close eye on.

Google has not put its g-mail servers in China, so that was a good step and it is something that should be continued. Really we are very cautious about it and we keep telling companies don't put your servers in internet restricting countries because that can put you in the situation where you would be forced to reveal the personal data, to give those data to the government. Again, we believe that local laws are less important than international standards in terms of protecting freedom of expression and international standards.

Harry talked of Cisco, and I think that there has been a lot of things said about Cisco, about how they have created this police net products and how they have been building the internet in China, and there is probably a need for more evidence and more information about how exactly the routers were set up to monitor not only -- I mean, to

monitor dissidents basically, so Cisco would be another one we really want to keep a very close eye on.

Mr. CALINGAERT. I would think of the issue in this term, that there is a marketplace for developing technologies, and part is marketized and part is nonprofit. I mean, some of the best anticensorship tools like Siphon were developed at universities. And rather than try to figure out, okay, what is the silver bullet here, let the market figure it out because I think a lot of American consumers are looking for the same kind of things as users in China, Iran or elsewhere. They want ease of use, they want security, they want privacy protected and so on.

So I would let the market sort of sort that out. Let the various companies compete to come up with the best technology, offer some public resources for the nonprofit efforts to develop areas of technology like anticensorship that have less market demand and then really focus on curbing the abuses, preventing the technology that can be used for censorship from getting to the repressive governments.

Mr. HOGREFE. Can I ask -- oh, I am so sorry, Harry. Go ahead.

Mr. WU. I wonder why so much of our talking about censorship, anticensorship marketing, government, company, whatever, what has happened to the Christmas bill, why you cannot pass it over. It is simply just passed over. Who blocked it? Who played a role in there to stop the bill? This is a major problem. Otherwise, well, Chinese today back up, say, well, this optional. Maybe one day come back at it again. Okay. So the Green Dam is one of the issue.

Mr. HOGREFE. Right.

Mr. WU. But until today there is nothing really free about it. Yes, I just don't want to talk about things. If you can pass the bill, that would be good. Thank you.

Mr. HOGREFE. Yes, absolutely, and I think that that is what we are all working on and push for, and Kumar highlighted some of the issues obviously that occurred in the U.S. Congress.

Let me just ask a final, and I know we have to close because we actually are about to be kicked out of the room, the latest line-up or addition to the line-up of search engines available in Chinese is Bing, right, the Microsoft service that was I understand just started like in the beginning of June. Do we have any information on if there is filtering going on, if you can get access to the Dalai Lama's website or something on Tiananmen Square, or is that too new a service and we don't know yet how that is working?

Okay. Well, maybe we will monitor that and see, you know, because hopefully given that they in essence launched a new service or of course based on their old technology but a new service as such under a new product name, maybe some of the discussions that have preceded or that someone is focused on Yahoo and Google could hopefully be taken into consideration as they develop this new network.

In any event, I wanted to thank all of you for coming and thank you so much for your testimony, and Elizabeth and I will continue to work on this. This is obviously not the last hearing that we will have.

Ms. HOFFMAN. Hopefully the next one will have some members.

[Laughter.]

Mr. HOGREFE. That is right. And hopefully we won't have 26 votes. But thank you again for coming.

[Whereupon, at 12:28 p.m., the Commission was adjourned.]